before the trial was to start, Ameritech had to expedite change orders changing the telephone numbers assigned to the AT&T placed orders.

105. Delayed Beginning. The agreement was to conduct a simple trial that could be concluded quickly. At the April 21 meeting, Ameritech proposed an expedited schedule. AT&T would not commit to an expedited schedule, and instead requested more data and kept attempting to expand both the scope and the scale of the trial. However, AT&T did not have the ability technically to submit the orders in the format they desired. For several weeks, AT&T refused to provide even an estimate of when it would be able to submit the trial orders. Finally, AT&T notified Ameritech that it would be able to submit orders on May 28.

106. Bogus ID. When the agreed-upon date (May 28) for AT&T to send the orders arrived, the orders did not. At this point in time, AT&T was using the EDI interface to send thousands of resale orders each week to Ameritech. AT&T claimed to have sent the trial orders, but no orders were electronically transmitted via the interface. Since communications exchanged using the EDI protocol produce for the sender an acknowledgement message with a unique number identifying the transaction, Ameritech requested that AT&T provide the acknowledgement identifier. AT&T admitted that the messages it purportedly had sent had never been acknowledged by Ameritech's EDI interface. Subsequent investigation with GE Information System ("GEIS"), which supplies the public data network connection used by Ameritech, discovered that attempts to transmit messages had been made under an unauthorized number. Without any advance notification or coordination with Ameritech, AT&T apparently had decided to use a new identifier,

which was viewed by the GEIS network as an unauthorized attempt to gain entrance to Ameritech's interface and therefore blocked. GEIS subsequently notified Ameritech of the attempt of an unauthorized user to access the interface. Ameritech asked AT&T to resubmit the orders using one of its two authorized IDs. AT&T informed Ameritech that it could not do so, since those IDs were being used by AT&T's production systems, and that the orders were being generated by a prototype system operated by an outside firm. Although the GEIS interface could be modified to send the transaction, additional security measures designed to protect AT&T and other users from unauthorized tampering with their customer accounts would still have prevented the orders from successfully being transmitted. Approximately two weeks are required to establish a new trading partner ID with the EDI system.

107. Therefore, on Friday, May 30th, Ameritech's EDI group proposed a plan to get the trial started. Working over the weekend, they developed a program to straddle the interface and change any incoming EDI orders being entered with AT&T's bogus ID to a valid ID associated with the production orders issued by AT&T. Because the EDI messages are sent in both directions, the program would also intercept the EDI responses sent from Ameritech to AT&T and, for all orders entered using the bogus ID, would replace the valid ID with the bogus ID before forwarding the message to AT&T. This software was written, tested and installed over the weekend, and AT&T was notified on Monday, June 2 that it could resubmit its orders.

108. AT&T's Network Interconnect Problems. In addition to the bogus ID problem mentioned above, the orders for the platform were further delayed due to network

interconnection problems between AT&T's EZ Link service and the GEIS network. These problems involved the interLATA services of GEIS and AT&T, and were resolved by them.

109. Change of Location. The original orders were submitted by AT&T for a given location within its building. Although not called for by the test protocol, the subsequent orders specified a different location within the same building. Because the AT&T building is a multi-tenant building, Ameritech was required to dispatch an outside technician to work the orders. AT&T offered no explanation as to why it changed the service location on the orders.

110. AT&T Withheld Critical Information on 900 Translations. AT&T had requested that the trial attempt to utilize a new and untested method for handling directory assistance (DA) calls. Under the standard routing algorithm, calls to 411 or 555-1212 from an unbundled line port could be directed, using custom routing, to a unique trunk group associated with AT&T's DA services. AT&T requested that instead of routing the calls to a DA trunk group, Ameritech translate 411 and 555-1212 calls to a unique 900 number associated with AT&T's DA services. AT&T subject matter experts attending a April 21 meeting assured Ameritech that other LECs had successfully implemented this procedure. Unfortunately, AT&T withheld from Ameritech critical technical details concerning the use of this feature in the 5ESS switch. Ameritech uncovered this problem while testing this configuration in its services integration laboratory in Hoffman Estates, Illinois. Among the dialing plans used in the Chicago area, an end user can dial an area code with the 555-1212 number. For instance, a Chicago user can dial 1+312+555-1212 to reach directory assistance. The problem is that the 5ESS switch is capable of translating only seven of the

ten dialed digits. Ameritech notified AT&T of this problem. Ameritech then received a request from AT&T to establish a conference call with an AT&T technical expert in New Jersey to discuss the problem. The AT&T personnel admitted that they were familiar with the problem and had encountered it before. They offered no explanation as to why they withheld this information.

111. Lost 865 Order Confirmations. AT&T notified Ameritech that it was unable to locate EDI 865 transactions (Order Completion Notification) and suggested that the system had not sent them. Upon further discussion with AT&T personnel, it was discovered that AT&T's practice was to place all 865s in a large cardboard box, and that AT&T personnel involved were not notified that the 865s associated with the test orders were to be pulled out for special treatment.

112. Invalid Testing Procedures. AT&T technicians were observed testing lines by dialing only a 01 without any subsequent digits on test calls. The digits 01 are used with international direct dial calls, and indicates to the switch that additional digits associated with the international number will be dialed. If no additional digits are dialed within a reasonable period, the switch times out and the call is sent to a recorded message. This was not one of the test calls agreed to by the trial team and the AT&T technician tried to record the call as a failed attempt. In fact the switch acted exactly the way it should have and the treatment was correct for an abandoned international direct dialed call.

C. The MCI Trial

113. On April 24, 1997, Ameritech and MCI agreed to conduct a trial of the "platform" similar to the one being conducted with AT&T. The parties agreed to test the "platform" lines in both Illinois and Ohio, which had been ordered through Ameritech's AIIS unit using the Unbundling Questionnaire, and concurred that Ameritech would produce a Daily Usage File. On May 8, 1997 Ameritech received the completed orders for the ULS line port and unbundled loop combination. On May 9, 1997 Ameritech began to build the required LCCs, and on May 16, 1997, the lines were successfully installed. On June 12, 1997, Ameritech and MCI agreed to a list of test calls to be made from the lines. The same evening, Ameritech and MCI made the test calls on the Illinois line involved in the test. All calls were completed as expected. Subsequently, Ameritech forwarded the Daily Usage File containing the test calls data to MCI.

114. As opposed to the AT&T trial, the platform test with MCI was completed in a little over a month, and promptly demonstrated that the service can be ordered, provided, and billing data provided. This shows what can be done when both parties cooperate, rather than when one party seeks to delay the trial and have it fail to further its legal position.

115. This concludes my affidavit.

I hereby swear, under penalty of perjury, that the foregoing is true and correct, to the best of my knowledge and belief.

Daniel J. Kocher

Subscribed and sworn before me this 3rd of July, 1997.

"OFFICIAL SEAL"
Debra A. Busam
Notary Public, State of Illinois
My Commission Exp. 04/24/2001

Notary Public

My Commission expires: _____

reseller or requesting carrier whose customer originates the operator services or directory assistance request.

Q. Is this capability currently available from your OS and DA platform?

A. Yes.

Q. AT&T claims that Ameritech Illinois can use AIN triggers to provide custom routing. Is it technically feasible today to use AIN to support selective routing of OS/DA calls?

A. No, it has not yet been developed or tested. At a theoretical level, AIN might be used to perform selective routing of OS/DA calls. At a more detailed level, carriers need to be aware that based upon today's technology there are various serious limitations for this approach. For example, AIN triggers are not able to distinguish between OS/DA calls and other calls. This means that all calls (with a few exceptions), not just OS and DA calls, made by a customer would encounter an AIN trigger and the associated query/response delay. This means all calls from the carrier's customer would encounter the delay and cost of the AIN processing, even though only relatively few calls would actually be OS and DA calls.

Another example of a limitation on the use of AIN for selective routing is that since nearly all calls from the carrier's customers would encounter the trigger, any failure of the signaling network or AIN application might block those customers' ability to place nearly any call. For cases of signaling or AIN failures, the switch includes an "escape list" that allows a small number of specific numbers to "bypass" the AIN trigger. This is used to ensure that

calls to 911, etc., can be completed regardless of signaling or AIN failures. There exists only one "escape list" for an entire switch. If the switch is shared by multiple carriers, there would need to be a process to administer the single list, as well as the recognition that the escape list allows some calls not to encounter the AIN selective routing service for OS and DA calls.

Q. Would the use of AIN for selective routing of OS and DA calls interfere with other services the carrier might want to offer?

A. Yes. Requesting carriers should recognize that AIN interacts poorly with some switch-based features. This means that some switch based services either would not function at all, or might operate in unexpected fashions for customers assigned an AIN trigger for the purpose of providing selective routing of OS/DA calls. Examples of features that might be adversely impacted are CLASS features such as Automatic Callback and Automatic Recall. Carriers also need to recognize that the use of an AIN trigger for selective routing of OS/DA calls prevents the use of that trigger for other AIN services the carrier might want to offer to that customer. For instance if a carrier were to use an off hook delay trigger for selective OS/DA routing, that customer might not be able to use Ameritech Call Control, which also requires the use of the off hook delay trigger.

Q. Will Ameritech Illinois support the use of AIN for selective routing of OS and DA calls?

A. Yes. This is exactly the purpose for which Ameritech Illinois is providing an SCE offering and an SMS offering. Carriers that desire to develop unique service capabilities based upon AIN have the ability to develop their own AIN

applications which would be loaded on Ameritech Illinois' SCP, and would be assigned to that carrier's customers.

Q. AT&T also asserts that ASI proxy can be used to provide selective routing. Does Ameritech Illinois support the use of an Advanced Service Interface (ASI) Proxy solution for the selective routing of OS and DA calls?

A. No, at this time AT&T does not provide sufficient information regarding its proposal for Ameritech Illinois to determine if it is technically feasible now, or if the capability could be developed to provide selective routing. Ameritech Illinois has only limited knowledge of ASI Proxy capabilities. Ameritech briefly experimented with Proxy capabilities in an evaluation of voice dialing service. We do not currently have such capabilities available in most Ameritech Illinois' switches, and we would need to determine whether we need to add necessary supporting hardware and software in our network for this solution. (We do not presently have any Intelligent Peripherals in our network, for example.) We do not believe the Proxy capability can be used for selective routing of Operator Service calls. Our limited understanding of Proxy is that it cannot be used to route to a trunk group, which would be necessary to ensure calls to OS systems are routed on trunks supporting signaling suitable for OS services. Proxy might be capable of supporting selective routing for Directory Assistance (DA) services. We know there are interworking issues between Proxy and other services, including AIN, that would need to be understood and resolved. We would need to understand more about Proxy capabilities before we could review whether Ameritech Illinois could support this approach for selective routing of DA calls.

SUPPLEMENTAL REBUTTAL TESTIMONY OF WAYNE HEINMILLER ON BEHALF OF AMERITECH ILLINOIS

Q. Please state your name and business address.

A. My name is Wayne Heinmiller. My business address is 2000 W. Ameritech Center Drive, Room 4C65D, Hoffman Estates, Illinois 60196.

Q. By whom are you employed?

A. I am employed by Ameritech Services, Inc.

Q. Are you the same Wayne Heinmiller who previously testified?

A. Yes I am.

Q. What is the purpose of your testimony?

A. My purpose is to respond to the supplemental direct testimony of Staff witness Graves and his discussion of the of using AIN network capabilities to selectively route OS/DA traffic.

Q. Mr. Graves states that "Ameritech has not addressed the possibility of an AIN solution to the issues of OS/DA unbundling and branding." (ICC Staff Exhibit 7.00, page 9) Has Ameritech Illinois addressed this possibility in this proceeding?

A. Yes. My rebuttal testimony specifically addressed using AIN to address OS/DA unbundling and branding; demonstrated that there are serious limitations to using AIN to address OS/DA unbundling and branding; and indicated that Ameritech Illinois has made its AIN Service Creation and Service Management capabilities available to other carriers. These carriers can use these capabilities to develop their own OS/DA routing and branding capabilities if they believe that AIN is a suitable solution for them.

Q. Mr. Graves indicates that "access to AIN triggers" is an issue to be investigated further. (ICC Staff Exhibit 7.00, pages 10-12) Does Ameritech Illinois provide access to its AIN triggers to other carriers?

A. Yes. Through Ameritech Illinois' current AIN offerings (AIN Service Creation, AIN Service Management, Unbundled Access to AIN Applications), other carriers can develop AIN services and offer those services to their customers using AIN triggers in Ameritech Illinois' unbundled switching elements. Under these offerings, AIN services developed by other carriers are subjected to the same test process as Ameritech Illinois' AIN services, and are deployed and operate on Ameritech Illinois' Service Control Points (SCPs).

Q. Does Ameritech Illinois allow carriers to connect their Service Control Points (SCPs) to interact with AIN triggers in Ameritech Illinois' unbundled switching elements?

A. No. Ameritech Illinois' network does not presently incorporate the capability to support interconnection of other carriers' SCPs for AIN services. Ameritech Illinois has explained how we believe that doing so would present unacceptable risks to all carriers and end users that rely on Ameritech's network. AIN technology was not developed anticipating interconnection among carriers, and Ameritech Illinois believes that new or different functionality is needed in order to support interconnection of other carriers' SCPs to provide AIN services. Historically, the functionality to protect Ameritech Illinois' network and those of other carriers, while allowing interconnection of other carriers' SCPs, has been referred to as "mediation" or "mediated access". The need to protect networks when interconnecting is not unique to AIN. For example, interconnection functions that protect interconnected networks are referred to as "firewalls" and "gateways" for the Internet. Home personal computer users are also recognizing the need to protect their PCs when they interact with sites on the Internet.

Q. Mr. Graves asserts that an inquiry is needed to address the possibility of using AIN triggers. Is the interconnection of AIN networks being addressed by the industry?

A. Yes. There are at least two industry forums working on this issue. The IN Forum and the Network Interconnection/Interoperability Forum (specifically the Network Interoperability Architecture Committee or NIAC) are both actively working on this issue, continuing work that had been begun by the Information Industry Liaison Committee (IILC). There are also various activities and actions underway

800 East Cook Street
Floor 1E
Springfield, IL 62721
Office 217/789-5174
Fax 217/789-5223

Terry R. Henkel
Director
Regulatory Affairs

July 31, 1996

To: Ms. Donna Caton
Chief Clerk
Illinois Commerce Commission
527 East Capitol Avenue
Springfield, Illinois 62794-9280

The accompanying three reports and accompanying attachments are being issued by Ameritech Illinois and are transmitted to you for filing.

These reports were previously provided to the Commission's Staff on July 26th., 1996 along with Ameritech Illinois' wholesale tariff filed in compliance with the Commission's Order in Docket Nos. 95-0458 and 95-0531 consolidated. Ameritech is submitting these reports in compliance with the Commission's Order. These reports detail Ameritech's compliance or plan for compliance relative the following requirements of the Order: offering of operational interfaces to resellers; offering of unbundled Operator Service (OS) and Directory Assistance (DA) and branding of OS and DA service (with reseller's name); and providing access to Ameritech's Advanced Intelligent Network (AIN) triggers.

Any questions may be directed to Jaime Villasenor, Director Regulatory Affairs. You may reach him at:

Ameritech Illinois
225 West Randolph Street, 18F
Chicago, Illinois 60606
Tel. No.: 312-727-5114
FAX No.: 312-727-4771

Sincerely,

(Signed) Terry Henkel
Director - Regulatory Affairs

DIRECT ACCESS TO AIN TRIGGERS

I. Introduction

In its Order dated June 26, 1996 in consolidated Docket Nos. 95-0458 and 95-0531, the Commission required Ameritech to provide direct access to AIN triggers, subject to the condition (inter alia) that if Ameritech Illinois "is not able to comply with the requirement ... on a basis that eliminates possible harm to the network, it must submit a full explanation and showing in support thereof with its compliance tariffs ...." Order, at 47. The purpose of this report is to demonstrate to the Commission that compliance in a manner that eliminates possible harm to Ameritech Illinois' network, and to those of interconnecting carriers, is not possible, and to submit the following materials explaining why compliance is impossible at the present time.

The provision of direct access to AIN triggers in such a manner as to eliminate possible harms to the network is not technically feasible, as recognized by various industry fora, including the Information Industry Liaison Committee ("IILC"), the Network Reliability Council, and the I/N Task Group. Over the past five years, the FCC has compiled a substantial record investigating many aspects of Intelligent Network deployment and unbundling, including the possible effects of direct trigger access. See, generally, In the Matter of Intelligent Networks, FCC Docket No. 91-346; copies of selected materials from that ongoing proceeding are provided as attachments hereto, and additional materials from that proceeding will be provided to the Commission and other parties upon request. In addition, for

reference purposes, a description of Ameritech's implementation of AIN is provided as Attachment 1.

Ameritech is currently developing several alternative arrangements which meet the needs expressed by the Commission and also minimize the associated risks to the network. Ameritech will consider the provision of other such arrangements in response to bona fide requests (as contemplated by the Telecommunications Act of 1996) for interconnection to AIN capabilities.

II. Direct access to AIN triggers without risk of network harms is not technically feasible.

Ongoing industry-wide efforts have demonstrated that the provision of direct access to AIN capabilities in a manner which eliminates the risk of network harms is not technically feasible. The provision of such direct access would pose unavoidable risks to the networks of Ameritech Illinois, and those of interconnecting carriers, in the areas of network security and management, unpredictable feature interactions, and customer billing and privacy. As noted on the FCC's record in its Intelligent Networks proceeding (see Attachment 2, which provides a compilation of specific instances in which adverse consequences would result from direct access), these risks are as broad in scope as they are inherently unavoidable.

A. Network security and management

Direct access to AIN triggers by interconnecting carriers would pose an unavoidable threat to network security and reliability. The reason this threat is unavoidable as well as serious is the fact that AIN triggers are a component of the

operating software of the central office switch itself. As such, AIN triggers enable immediate manipulation of all individual calls being handled by a switch.

The obvious consequences of permitting direct access to such capabilities would flow from the loss of single-carrier accountability for overall switch integrity. If other providers were given direct access to AIN triggers, their individual actions could seriously impair the switch's coordination among network elements controlled by the operating software. For example, AIN enables multiple calls to be re-routed on a real-time basis to account for shifting traffic volumes and patterns within the switch; thus, uncoordinated call-handling actions taken by interconnected carriers with direct trigger access could set in motion a chain reaction of software efforts to control and balance the rapidly-changing traffic patterns resulting from such unexpected shifts. Moreover, a single interconnected carrier's inability to handle or receive calls could result in the termination, based upon AIN triggers, of calls which may have involved other service providers' use of the same triggers. In this way, other carrier's customers would experience call cutoffs and unexpected feature inoperability. Such a situation would also clearly introduce the potential for unauthorized rerouting by a carrier of calls placed by customers of another carrier. A summary of the related issues under consideration by the FCC can be found in a recent Ameritech filing regarding switching equipment capabilities related to direct AIN interconnection (see Attachment 3).

A useful parallel for purposes of this proceeding can be found in the recent history of SS7 network-related failures. Modern networks (as operated by both LECs and IXCs) rely heavily on the signaling capabilities of the SS7 network. Not only

does the SS7 network support IN services (e.g., 800, 911, LIDB), AIN services, and other services (e.g., CLASS, Caller ID), but it is also used for the basic processing that allows calls to be processed from one switch to another (trunk signaling). As developed in wireless networks, SS7 is often used to pass messages that track users as they move within and between networks.

As recent experience demonstrates, failures of SS7 networks can have far-reaching impacts. In January 1990, AT&T experienced an SS7 problem which caused a significant portion of their network to simply stop processing calls. It took approximately 9 hours to identify and correct the problem. In June 1991, Bell Atlantic experienced SS7 network problems which affected 5-6 million customers (including Washington DC) for up to 9 hours, while Pacific Telesis had problems affecting 3 million customers (Los Angeles) for 2 to 3 hours. In July 1991, Bell Atlantic experienced a problem, related to their June outage, which disrupted calling for over 1 million lines in the Pittsburgh area. During these failures, affected customers of Bell Atlantic and Pacific Telesis were blocked from completing intraLATA calls from one switch to another.

Each of these network failures was caused by minor bugs in software that had received extensive testing. In the case of the AT&T outage, one routine in the SS7 software in their 4ESS tandem switches was identified as the root problem. In the case of the Bell Atlantic and Pacific Telesis failures, an error in a single byte of the software generated the problem.

Partly as a result of these outages, the companies that participate in the Network Operations Forum (NOF) established an Internetwork Interoperability Test

Plan (IITP) to create a process for testing and verifying the interconnection of SS7 networks. There was concern that these kind of problems might be able to spread from one company's SS7 network to another. The interconnection testing process identified by the IITP is still used today when SS7 networks connect. This recent SS7 experience clearly illustrates both the catastrophic nature and the character of the problems that could occur if direct access to AIN triggers were implemented.

B. Feature Interaction

In addition to overall network security and management effects, direct access to AIN triggers would pose an entirely new category of network harms resulting from the unanticipated effects between the AIN-based services created and deployed by interconnecting carriers given such access. For example, if one provider used a trigger to treat all calls to a given NPA-NXX in a specific manner (e.g., routing to a particular IXC) and another provider used the same trigger to treat calls to a specific telephone number within that NPA-NXX (e.g, forwarding them to a service platform located elsewhere), calls placed by customers of both carriers would reach unexpected destinations and services. Even assuming that service-by-service coordination were possible among multiple providers with direct trigger access, the impact of new features introduced by any one carrier could not be predicted with certainty; unanticipated failure of existing features or services would be a likely result.

C. Customer billing and privacy

The use of AIN triggers involves the real-time transmission of information related to call progress and duration, as well as customer feature complement, line

status and configuration. Such information falls squarely within the new Telecommunications Act's definition of Customer Proprietary Network Information ("CPNI") as "information related to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service ..." Telecommunications Act of 1996, Section 222(f)(1)(A). No technical solution exists in the software of any switch vendor to restrict a particular carrier to access to the CPNI of its own customers. As a consequence, providing direct access to AIN triggers would render impossible compliance with the Act's requirement that carriers safeguard the CPNI of its customers and those of other carriers, as specified in Sections 222(a) and (b) of the 1996 Act.

In addition, many AIN applications are capable of changing billing parameters which indicate the proper assignment of responsibility for charges incurred on a given call. Since no provisions exist in any vendor's existing switch software for verification of the accuracy of such billing information, unauthorized alterations of the billing parameters could not be detected or prevented. Moreover, the above-mentioned ability of a carrier with direct trigger access to reroute traffic within a given switch presents clear potential for the undetected diversion of traffic properly routed to other carriers.

III. Ameritech is developing other service arrangements which meet the needs expressed by the Commission without introducing the risks of direct trigger access.

Acknowledging the validity of the Commission's goals of "promot(ing) innovations with respect to service offerings," Ameritech is currently developing

new service arrangements which will permit other carriers to conceptualize, create, deploy and manage new AIN-based services in Ameritech Illinois' network while minimizing the service risks that would result from direct trigger access. These arrangements, known collectively as the AIN Service Management Systems Service Creation Environment ("SMS/SCE"), will enable other service providers to develop and test new AIN-based services in a fully-functional laboratory environment prior to deployment, thus permitting complete and effective testing for feature interactivity and service reliability before deployment in the networks of Ameritech Illinois and other affected providers.

SMS/SCE will be offered in a nondiscriminatory manner to requesting carriers on a negotiated, service-specific basis. Each negotiated offering will be predicated on cost-sharing arrangements and market demand forecasts, subject to AIN platform capabilities. Future SMS/SCE service offerings will likewise be selected for development based on market demand forecasts and platform capabilities.

SCE/SMS will enable other service providers to manage current AIN service offerings for their customers connected to an Ameritech Illinois end office. It will also enable other service providers to differentiate their products from those of Ameritech Illinois by creating unique new services for their customers. AIN services developed and tested via SMS/SCE will be fully compatible with all elements of Ameritech Illinois' network. Service software will be loaded, tested, and diagnosed within Ameritech Illinois' network by Ameritech Illinois. Service providers using the capabilities of SMS/SCE will have modification, provisioning &

service management functionality (for managing their newly-deployed services) equivalent to that of Ameritech Illinois.

Service provider requests for interconnection of their SSPs to Ameritech Illinois' SCPs for AIN services will be considered and negotiated on a service-by-service basis because of the technical limitations & complexities of managing privacy issues, feature interactions, network management control issues, etc., in a multi-provider environment. Gateway screening, signaling traffic restrictions and service logic restrictions are examples of the types of precautions that may be implemented for any given service to minimize possible risks to the network and to customer service. Compatibility testing of any such AIN services with the SSPs of multiple providers will be done jointly between Ameritech Illinois and the interconnected service providers.

If so requested by a provider using the capabilities of SMS/SCE, Ameritech Illinois will internally develop new, unique service concepts for other service providers, will work jointly with other providers' development personnel, or will allow service providers to develop new, unique service concepts on Ameritech Illinois' SCE platform within the technical limits of that environment.

Since the overall configuration of SMS/SCE is still evolving, specific pricing and service arrangements are not yet defined. At a minimum, some or all of the following pricing elements may be included in determining an appropriate price for the AIN SCE/SMS Interconnection offering (inclusion of specific elements would vary depending on the specific service under consideration):

Service Creation
Service Development

Service Development Consulting
Service Integration Laboratory ("SIL") testing
Field Testing
Provisioning
SMS Access
SMS Utilization
SS7 Network Resource Utilization
SCP Processing
Queries
Announcements
Additional call legs
Maintenance (Includes trouble reports)

The determination of how each of these elements would be treated in a specific instance (i.e., recurring or non-recurring charges, flat rated or usage sensitive, etc.) is yet to be determined and may be negotiated on a service by service basis.

In addition to the development of SMS/SCE capabilities as described above, Ameritech Illinois will consider other AIN interconnection arrangements as requested by carriers submitting a Bona Fide Request ("BFR") for such arrangements. A BFR is the vehicle proposed by Ameritech to the FCC for carrier requests for AIN Interconnection (see Attachment 4, at p. 29 for a full description of this process). This process is patterned after the one adopted by the Commission for requests for so-called "sub-loop unbundling" (83 Ill. Admin. Code, §790.320(b)).

To enable Ameritech to provide a complete, timely and thorough response, a BFR should include, at a minimum: (1) a complete technical description of the requested service arrangement, (2) estimated demand/quantity for the service, (3) a commitment to purchase the service or provide funding for the processing and development costs incurred by Ameritech in responding to the request.

ATTACHMENT 1

AIN evolved from Intelligent Network (IN). Both AIN and IN use similar network architectures, and similar terminology. Both AIN and IN co-exist within Ameritech's network. The distribution of functionalities between network components differ slightly between AIN and IN. The key component present in both AIN and IN architectures is the Service Control Point (SCP), a system connected to the Signaling System 7 (SS7) network. (Signal Transfer Points, or "STPs", route messages among the nodes of the SS7 network. SS7 is used for other capabilities as well, including trunk signaling and CLASS services.) A switch which is able to communicate with an SCP is a Service Switching Point ("SSP"). A switch may be both an IN and AIN SSP, or it may be equipped to serve as only one or the other. Switches that are not SSPs are configured to route calls for IN and AIN services to a switch that is contains appropriate SSP capabilities.

For IN services, the software in the switch creates a "query" message when it determines that a specific service requires information from an SCP. The query message is transmitted by the switch into the SS7 network, where it is routed to the appropriate SCP by the signaling functions of an STP. At the SCP, the information request contained in the query message is analyzed, and the requested information is retrieved. The SCP formulates a "response" message, which it transmits back to the switch through the SS7 network. When the response is received by the switch, the information in the message is analyzed, and the processing of the call continues using the information provided by the SCP.